imation

DEFENDER™ F200+BIO USER GUIDE

Contents

Introducing Defender™ F200+Bio 2
Minimum System Requirements 2
Imation Documentation 2

Getting Started 4
Opening and closing a device 4
Attaching the lanyard loop 4
Personalizing a device 6

Accessing data on the device 8
Logging into and out of the device 8
Saving and opening files 9
Disconnecting the device 9

Troubleshooting 10

Warranty Information 12

INTRODUCING DEFENDER™ F200+BIO

Defender™ F200+Bio is a USB (Universal Serial Bus) portable flash drive with built-in biometric security and data encryption.

Figure 1-1: Defender F200+Bio

This guide is designed to help you set up your Defender F200+Bio device with minimal effort.

MINIMUM SYSTEM REQUIREMENTS

Defender F200+Bio comes with built-in Imation Defender ACCESS Standard™ software on its application partition. The following list describes the requirements you need to use your device with ACCESS Standard.

- A USB port (Type A)
- An operating system that supports USB 2.0 or 1.1 Mass Storage Devices

Operating systems

- Microsoft Windows 7
- Windows XP Pro SP2
- Windows XP Pro SP3
- Windows XP Home SP3
- Windows Vista (Home, Business and Enterprise editions SP2)
- Mac OS X 10.5 and 10.6

IMATION DOCUMENTATION

You can find detailed instructions about using and managing Defender F200+Bio in the *ACCESS Standard User Guide*.

Topics include:

- Information about Imation Defender Collection Devices
- Personalizing the device
- Accessing the device
- Managing users

INTRODUCING DEFENDER™ F200+BIO*cont.*

- Managing devices
- Protecting the device from viruses
- Troubleshooting

Online Help is also available with ACCESS Standard software.

To view the ACCESS Standard User Guide

- From the root directory of the application partition, double-click the **UserGuide.pdf** file.

Note: You need Adobe® Reader® (http://www.adobe.com/acrobat) to view the documentation.

To view online Help

- When ACCESS Standard is open, click **Help** on the page for which you want more information.

GETTING STARTED

OPENING AND CLOSING A DEVICE

Defender™ F200+Bio has an integral case that opens by removing a large front cap. .

To open a device

- Grasp the front and rear caps and pull apart.

To close a device

- Slide the device into the front cap and squeeze the caps together.

ATTACHING THE LANYARD LOOP

Defender F100 and Defender F150 come with a lanyard loop that allows you to attach it to lanyards or other objects.

To attach the lanyard loop (optional)

1. Insert the small threaded end of the lanyard through the hole in the main part of the device.

GETTING STARTED *cont.*

2. Grip both ends of the lanyard loop and bend the ends towards each other in a circle.

3. Insert the small end into the larger barrel.

4. Turn the larger barrel to thread the parts together.

5. When the small bullet is completely inside the larger barrel, the loop is secure and ready for use.

GETTING STARTED*cont.*

To remove the lanyard loop

1. Turn the barrel (counter-clockwise) to loosen the small bullet.

2. When the small bullet is completely separated from the larger barrel, pull the lanyard loop apart.

PERSONALIZING A DEVICE

When you plug in a new device, you must personalize it before you can use the authentication and private partition features. The device uses pre-installed ACCESS Standard software to guide you through the personalization process. ACCESS Standard starts automatically when you plug in a new (or recycled) device. If autorun is not configured for your computer, you can start ACCESS Standard from the application partition on the device.

Personalizing a device involves three main steps:

1 **Applying a device profile**—The profile sets default preferences for the device. You can choose the Typical profile with preconfigured device settings, or the Custom profile that allows you to configure device settings. The Typical profile contains the following device settings:
- Authentication method: Biometric only
- Number of device users: 1 (not including the Administrator)
- Private partition uses the total available disk space
- Two Factor authentication: Off
- Biometric Security Level: 1 in 4,500
- Minimum password length: 6
- Password Retry Limit: 10
- Password Re-use Threshold: 3
- User Rescue: Enabled
- Data Destruction: Off
- Administrator Account: Enabled
- Biometric Retry Limit: Infinite

2. **Creating the Administrator account**—Only the Administrator can perform certain operations on a device, such as adding, removing, and rescuing users. During the personalization process, the Administrator account is created automatically when you set the Administrator password. If you choose a Custom profile and disable the Administrator account, you will not be prompted to provide an Administrator password. In this case, you cannot create the account at a later time.

   It is very important that you memorize the Administrator password or store it in a safe place.

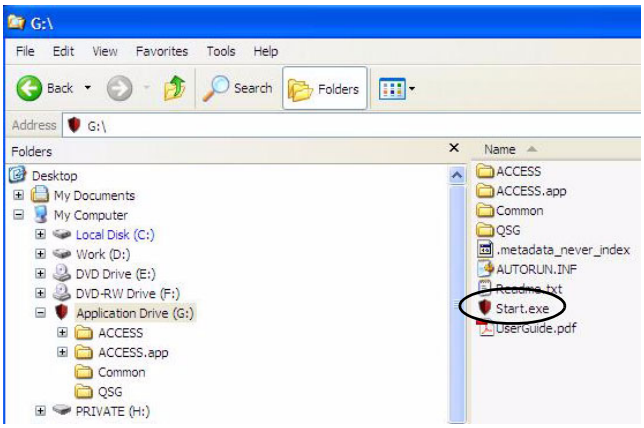
3. **Creating users**—Depending on the device profile, you can create one or more general users on the device.

GETTING STARTED*cont.*

To personalize the device

1. Plug the device into the USB port of the computer.

   If Autorun does not automatically start ACCESS Standard, double-click the **Start.exe** file from the root directory on the application partition. (If necessary, in the notification area at the far right of the taskbar, click the Imation Defender icon, and then click **Personalize Device** from the menu.)



2. On the initial ACCESS Standard page, click **Personalize Device**.
3. On the **Device Personalization** page, click one of the device profile options.
4. Complete the instructions on the pages that follow to set the Administrator password (if applicable) and create a user.

Note 1: If you do not complete the personalization process you may have to repeat some of the above steps the next time you connect the device. For more information about the personalization process, see the *ACCESS Standard User Guide*.

Note 2: After you successfully complete the Personalization process, you can access your private partition using a file manager. For more information about logging in and saving files to or opening files from the private partition, see "Accessing data on the device" on page 8.

ACCESSING DATA ON THE DEVICE

After you personalize a device, only registered users can authenticate to it. Authentication involves logging into the device using a password, fingerprint, or both. The authentication method you must use depends on the capabilities of the device and the profile applied to the device.

After you successfully log in, you can save files to, and open files from, your private partition. It is recommended that you log out of your device if you must leave it connected while you are away from your computer. Otherwise, another user could access your private partition while you are absent. You can also disconnect the device completely to bring the data with you.

This chapter provides information about the following topics:

- Logging into and out of the device
- Saving and opening files
- Disconnecting the device

LOGGING INTO AND OUT OF THE DEVICE

To log into the device

1. From the notification area, at the far right of the taskbar, right-click the Defender icon and click **Login**.
2. If you are using a computer running Mac OS X, open a file manager and click the application drive for the device. Double-click the **ACCESS Standard** application.
3. On the main page of ACCESS Standard, under **Manage Device**, click **Login**. Follow the prompts in the authentication wizard until the device successfully authenticates you.

Tip: If your device uses only biometric authentication, you can log into it without starting ACCESS Standard by swiping your finger across the fingerprint sensor.

To log out of the device

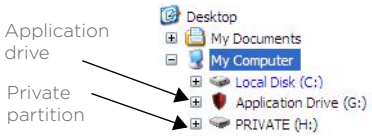
1. From the notification area, at the far right of the taskbar, right-click the Defender icon and click **Logout**.
2. If you are using a computer running Mac OS X, open a file manager and click the application drive for the device. Double-click the **ACCESS Standard** application.
3. On the main page of ACCESS Standard, under **Manage Device**, click **Logout**.

Tip: You can also log out of your device by right-clicking the Defender icon, and then clicking **Eject Device**. For more information, see “Disconnecting the device” on page 9.

ACCESSING DATA ON THE DEVICE *cont.*

SAVING AND OPENING FILES

When you plug in your device both the application drive and the private partition display in a file manager, such as Windows® Explorer, with an associated drive letter for each partition.



Once you log into the device, you can open files on your private partition using the appropriate program or a file manager. When you save data to your private partition, the device encrypts the data using hardware-based AES 256-bit encryption. Data is automatically decrypted when you open the file.

Note: You cannot save data to or delete data from the application partition.

DISCONNECTING THE DEVICE

To disconnect the device

- From the notification area at the far right of the taskbar, right-click the Defender icon and click **Eject Device**.

  If you are using a computer running Mac OS X, drag the device drive on the desktop to the **Trash**. Release the mouse button when you see the **Eject** prompt.

Tip: You can also disconnect the device by clicking the **Safely Remove Hardware** icon in the notification area at the far right of the taskbar. Click the message "Safely remove USB Mass Storage Device - Drive (F:); where F is the letter of the drive in the file manager that is associated with the device. Disconnect the device when the following message displays, "The USB Mass Storage Device can now be safely removed from the system".

Caution: Disconnecting the device either accidentally or on purpose, without properly ejecting it, could corrupt the data on the device.

TROUBLESHOOTING

If you experience difficulty using Defender™ F200+Bio after following the instructions in this User Guide, read the following troubleshooting information.

- Check to make sure the device is plugged in properly.
- Check the light emitting diode (LED) status of Defender F200+Bio.
- Check the Frequently Asked Questions section at Imation.com/support.

Table 4-1: LED states for devices

State	Description of state
Solid green	Open—if no authentication mechanisms are set, any user can use the device. User has logged into the device—if users exist, it indicates that the device has authenticated a user.
Flashing green	The flash frequency is approximately once per second and indicates that the device is waiting for a finger due to one of the following situations: • The device has just been plugged in and no user is currently logged into the device. • Software has initiated a biometric authentication or enroll operation. • A user has initiated a finger authentication operation for example, by touching the device when it is in the "idle" waiting-for-finger state. A device will remain in an idle state for only two minutes before the LED turns red to indicate the device is locked.
Flashing red once	Failed fingerprint authentication attempt. The device will go back to waiting for a finger (flashing green normal) after the failed signal finishes.
Flashing LED alternating between red and green	The device is waiting for a finger to authenticate but this is also the last chance to authenticate before biometric access is blocked. The frequency is approximately twice per second.
Flashing red	The device is either powering up or is totally blocked. When totally blocked, no authentication methods are available to allow a user to log into the device; this indicates that the device needs to be recycled.

TROUBLESHOOTING

cont.

Table 4-1: LED states for devices

State	Description of state
Solid red	The device is locked.
Blue LED	Indicates a data transfer activity for all devices.
Flashing red and blue	The device no longer has valid firmware.

Difficulty closing device cap

If the device cap is difficult to close, check the red rubber sealing ring on the main part of the device. If the ring is slightly twisted, use your fingernail to gently lift the ring and roll it out of the groove towards the USB connector—about as far as the LEDs. Then, roll the ring back into the groove. Repeat if necessary.

WARRANTY INFORMATION

Limited Warranty: If any defect in material or manufacture appears within 5 years of the date of original retail purchase of this product, it will be repaired or replaced at Imation's option. Proof of purchase is required to obtain warranty service. This warranty does not apply to normal wear or bundled software. Imation will not be liable for any lost data or other indirect, incidental or consequential damages. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to you. This warranty gives you specific rights - you may have other rights that vary from country to country.

Regulatory Compliance:

FCC

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Residential use statement:

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

—Reorient or relocate the receiving antenna.

—Increase the separation between the equipment and receiver.

—Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

—Consult the dealer or an experienced radio/TV technician for help.

Note: Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This Class B apparatus complies with Canadian ICES-003.

*The following information applies to only EU-member st*ates:

The equipment that you bought required the extraction and use of natural resources for its production. It may contain hazardous substances that could impact human health and the environment. The crossed-out wheeled bin symbol indicates that this product may not be treated as household waste. By disposing of this product using the appropriate take-back systems, you will help prevent the spread of hazardous substances to our environment and reduce the impact on natural resources. Those systems will reuse or recycle most of the materials of your end-life equipment in a sound way. If you need more information on the collection, reuse and recycling systems, please contact your local or regional waste administration.

Imation Enterprises Corp.
1 Imation Way
Oakdale, MN 55128-3414 USA

www.imation.com | info@imation.com

Imation, the Imation logo, Defender and the Defender Collection logo are trademarks of Imation Corp. ACCESS Standard is a trademark of MXI Security. All other trademarks are the property of their respective owners.

Copyright 2010 Imation Corp.